UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/919,960	08/02/2001	Bruno Couillard	35997-215056	4262

26694 7590 08/31/2007

VENABLE LLP
P.O. BOX 34385
WASHINGTON, DC 20043-9998

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2137	
MAIL DATE	**DELIVERY MODE**
08/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/919,960	COUILLARD, BRUNO	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,10-12 and 14-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,10-12 and 14-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-8, 10-12, and 14-31 are pending.

2. Amendment filed 07/13/2007 has been received and considered.

Claim Rejections - 35 USC § 112

3. The rejection of claims 24 and 25 under the second paragraph of 35 U.S.C. 112 have been withdrawn based on the filed amendment.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-8, and 15-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davies et al. (Security for Computer Networks) in view of Arnold (US 6148400).

As per claims 1-3, and 15, Davies et al. discloses transferring a first root key between a key provider system and

a second other system via an information network comprising the steps of: a) encrypting the first root key using a first super-root key of the key provider system (see pages 160 and 162 where the KKM encrypts the KK and the KKM is therefore the super-root key and the KK is the root key); b) providing within the second other system the second super-root key c) transferring the encrypted first root key from the key provider system to the second other system via the information network; d) providing the encrypted first root key to the processor internal to the first secure module of the second other system (see pages 162 and 163); and, e) executing program code on the processor internal to the first secure module to decrypt the encrypted first root key using the second super-root key stored wherein the first root key is useable for at least one of encrypting or decrypting private keys, and wherein a bit length of the first super-root key is greater than a bit length of the first root key, and said bit length of the first root key is greater than a bit length of any of said private keys being encrypted or decrypted (see pages 160-163).

Davies fails to explicitly disclose the use of a secure module in each of the systems with read only memory, and the keys only being accessible by the internal processor and the key

is other than modifiable and other than accessible outside the module.

However, Arnold teaches such a secure module (see column 8 line 49 through column 9 line 5).

At the time of the invention it would have been obvious to a person of ordinary skill in the art for each system of Davies et al. to contain a secure module.

Motivation to do so would have been to prevent tampering and eavesdropping (see Arnold column 8 lines 49-67).

As per claims 4 and 16-18, the modified Davies et al. and Arnold system discloses the processor internal to the module accesses the second encryption key only in response to a request from a corresponding secure module (as rejected above where it is implied that since the key is only used to encrypt other keys it wouldn't be used unless it is requested and as rejected in claims above).

As per claim 5, the modified Davies et al. and Arnold system discloses the use of an asymmetric pair, but fails to disclose the super-root keys are this pair. However, it would have been obvious to one of ordinary skill in the art that the use of a public key gives the advantage of only having to keep on key private.

As per claim 6, the modified Davies et al. and Arnold system discloses the super-root keys are symmetric (see Davies et al. page 160).

As per claims 7 and 8, the modified Davies et al. and Arnold system disclose generating keys within the system (see Arnold column 10 lines 43-64).

6. Claims 10-12 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Davies et al. and Arnold system as applied to claims 1, 6 and 15 above, and further in view of Spelman et al. (US 5680458).

As per claims 10, the modified Davies et al. and Arnold system fails to disclose second and third encryption keys being stored.

However, Spelman et al. teaches such keys (see column 2 lines 4-17 where the second and third keys are of the plurality of keys).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to store Spelman et al's keys in the modified Davies et al. and Arnold system.

Motivation to do so would have been to have more than one root key (see Spelman et al. column 2 lines 4-17).

As per claim 11, the modified Davies et al., Arnold and Spelman et al. system discloses encrypting a fourth encryption

key using one of the third encryption key and a key corresponding to the third encryption key; transferring the encrypted fourth encryption key from the key provider system to the second other system via the information network; providing the encrypted fourth encryption key to the processor internal to the first secure module of the second other system; and, executing program code on the processor internal to the first secure module to decrypt the encrypted fourth encryption key using the third encryption key stored within the memory circuit of the first secure module and to store the decrypted fourth encryption key within the memory circuit of the first secure module at a location corresponding approximately to the location where the second encryption key was stored (see Davies et al. and Arnold as applied to Spelman et al.'s key).

As per claim 12, the modified Davies et al., Arnold Spelman et al. system discloses replacing the second and third keys (see Spelman et al column 2 lines 4-17) and root key encrypting keys (see Spelman et al's keys as applied to Davies et al. and Arnold's key exchange system).

As per claim 14, the modified Davies et al., Arnold and Spelman et al. system discloses erasing the second encryption key from a first storage area of the memory circuit; and, storing the decrypted fourth encryption key within approximately

the same first storage area of the same memory circuit (see Spelman et al column 2 lines 4-17 where it is implied that a replaced key is erased).

7. Claims 19 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Davies et al. and Arnold system (alone or in combination with Spelman, Mason and Ehrsam) as applied to claims 18 and 25, and further in view of Easter et al (US 559889).

As per claims 19 and 26 the modified Davies et al. and Arnold system fails to disclose the module is FIPS 140 compliant.

However, Easter et al teaches such a compliant module (see column 6 lines 13-21).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to have the module of the modified Davies et al. and Arnold system be FIPS 140 compliant.

Motivation to do so would have been to allow for top security (see Easter et al column 6 lines 13-21).

8. Claims 20 and 27 rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Davies et al., Arnold and Easter et al system (alone or in combination with Spelman, Mason and Ehrsam) as applied to claims 18 and 26, and further in view of Bergum et al (US 5249277).

As per claims 20 and 27, the modified Davies et al., Arnold and Easter et al system fails to disclose a tamper detection circuit for erasing every cryptographic key stored within the memory circuit in dependence upon a detected attempt to access the electronic contents of the module in an unauthorized fashion.

However, Bergum et al teaches such a method of tamper protection (see column 4 lines 7-32).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to apply this method of tamper protection to the modified Davies et al, Arnold and Easter et al system.

Motivation to do so would have been to provide maximum key security (see Bergum et al column 4 lines 7-32).

9. Claims 21-24 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Davies et al., Arnold and Spelman et al system as applied to claim 10 above, and further in view of Mason et al (US 6331784).

As per claims 21-24 the modified Davies et al., Arnold and Spelman et al system discloses the claimed limitations as in claim 10 above, but fails to disclose the keys only being erasable by the program code.

However, Mason et al teaches a system with an erase only mode (see column 2 lines 39-47).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to incorporate Mason et al's erase only mode in the modified Davies et al., Arnold and Spelman et al system.

Motivation to do so would have been so no information can be read from the device (see Mason et al column 2 lines 39-47).

10. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Davies et al., Arnold, Spelman et al, and Mason et al system as applied to claim 24 above, and further in view of Ehrsam et al (US 4386234).

As per claim 25, the modified Davies et al., Arnold, Spelman et al, and Mason et al system fails to disclose the substantially non-volatile reprogrammable memory circuit is one of an electrically erasable read-only memory circuit and a random access memory circuit having an on-board power supply in the form of a battery.

However, Ehrsam et al teaches such a memory having a battery (see column 13 lines 45-50).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Ehrsam et al's

battery powered memory in the modified Davies et al., Arnold, Spelman et al, and Mason et al key exchange system.

Motivation to do so would have been to enable key retention when terminal power may not be present (see Ehrsam et al column 13 lines 45-50).

11. Claims 28-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Davies et al. and Arnold system (alone or in combination with Spelman and/or Mason) and further in view of Ober et al. (US 6307936).

As per claims 28-31, the modified Davies et al. and Arnold system (alone or in combination with Spelman and/or Mason) fails to disclose the exact ranges of key length (Davies et al. teaches the use of double keys to double the length and increase security).

However, Ober et al. teaches these specific lengths (see column 2 lines 47-60 and table 1).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use these specific key lengths.

Motivation to do so would have been to meet minimum security levels.

Response to Arguments

12. Applicant's arguments filed 07/13/2007 have been fully considered but they are not persuasive. Applicant argues that Arnold fails to teach a first secure module having a second super-root key within a read-only memory circuit; Davies teaches away from a combination with Arnold; Davies fails to teach the specific bit lengths claimed; and the remaining references fail to cure the above mentioned deficiencies.

With respect to Applicant's argument that Arnold fails to teach a first secure module having a second super-root key within a read-only memory circuit, Applicant is referring to Arnold (US 6175924), however, Arnold (US 6148400) was relied upon in the action mailed 03/13/2007 and remains relied upon for teaching this limitation. Specifically Arnold teaches ROM on a secure chip that contains a key (see column 8 line 49 through column 9 line 5) and it would be obvious for this ROM to store the super-root key of Davies in order to prevent tampering and eavesdropping. Therefore, the combination teaches a first secure module having a second super-root key within a read-only memory circuit.

With respect to Applicant's argument that Davies teaches away from a combination with Arnold because Davies teaches manual delivery of keys, Arnold teaches that the keys are added

during the manufacture of the chips (see column 8 line 49 through column 9 line 5). The chips containing the keys are then manually distributed to their respective locations. Therefore, both references teach the manual delivery of keys and do not teach away from a combination.

With respect to Applicant's argument that Davies fails to teach the specific bit lengths claimed, Davies teaches the idea that a key encrypting key should be twice as long as the key it is encrypting. Therefore, the length L of the KK (i.e. the root key) is twice as long as the key it encrypts. Furthermore, the KKM (i.e. the super root key) encrypts the KK of length L so it can be taken from this well-known teaching that the KKM is a key-encrypting key and therefore should be double the length of the key it is encrypting (i.e. 2L). Therefore, the KKM (i.e. the super root key) is longer than the KK (i.e. the root key), which is longer than the private key.

Applicant's argument that the remaining references fail to make up for the deficiencies of Davies and Arnold is moot in view of the above response.

Conclusion

13. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

Matthew D. Smithers
Matthew Smithers
Primary Examiner
Art Unit 2137